Methods and apparatus for enhanced security expansion of secret key into lookup table for improved security for wireless telephone messages

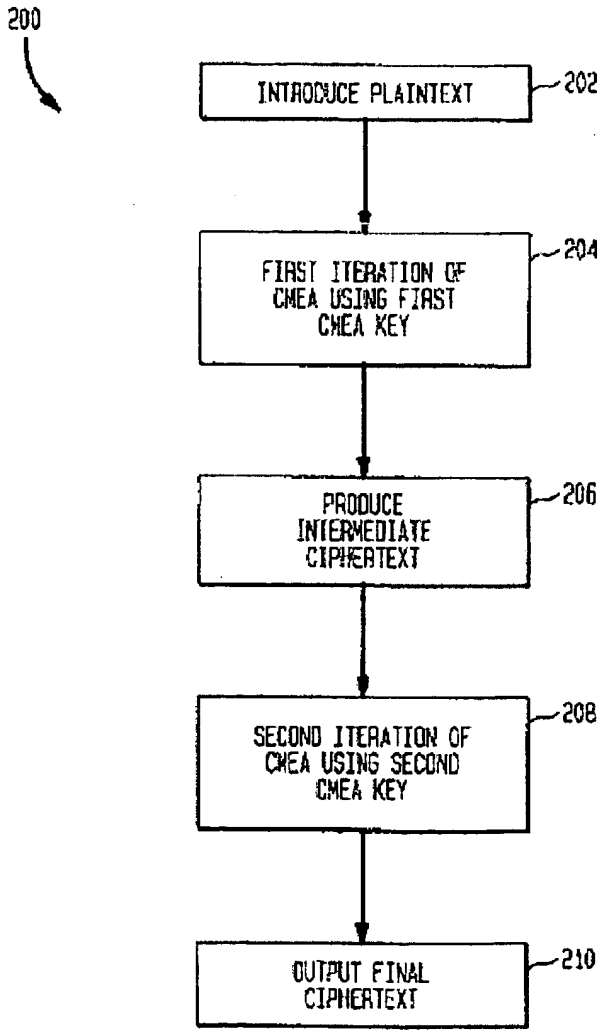
Patent number: CN1227021
Publication date: 1999-08-25
Inventor: ETZEL M H (US); FRANK R J (US); HEER D N (US)
Applicant: LUCENT TECHNOLOGIES INC (US)
Classification:
- international: H04L9/06; H04Q7/38
- european:
Application number: CN19980800620 19980414
Priority number(s): US19970043536P 19970414; US19980059107 19980413

Also published as:
WO9847262 (A3)
WO9847262 (A3)
WO9847262 (A2)
EP0914732 (A3)
EP0914732 (A3)
more >>

Report a data error here

Abstract not available for CN1227021
Abstract of corresponding document: **US6266411**

An enhanced CMEA encryption system suitable for use in wireless telephony. A plaintext message is introduced into the system and subjected to a first iteration of a CMEA process, using a first CMEA key to produce an intermediate ciphertext. The intermediate ciphertext is then subjected to a second iteration of the CMEA process using a second CMEA key to produce a final ciphertext. Additional security is achieved by subjecting the plaintext and intermediate ciphertext to input and output transformations before and after each iteration of the CMEA process. The CMEA iterations may be performed using an improved use of a tbox function which adds permutations to a message or intermediate crypto-processed data. Decryption is achieved by subjecting a ciphertext message to the reverse order of the steps used for encryption, replacing the input and output transformations by inverse output and inverse input transformations, respectively, as appropriate.



[19]中华人民共和国国家知识产权局

[51]Int.Cl[6]
H04L 9/06
H04Q 7/38

[12]发明专利申请公开说明书

[21]申请号 98800620.0

[43]公开日 1999年8月25日

[11]公开号 CN 1227021A

[22]申请日 98.4.14 [21]申请号 98800620.0
[30]优先权
[32]97.4.14 [33]US [31]60/043,536
[32]98.4.13 [33]US [31]09/059,107
[86]国际申请 PCT/US98/07823 98.4.14
[87]国际公布 WO98/47262 英 98.10.22
[85]进入国家阶段日期 99.1.11
[71]申请人 朗迅科技公司
地址 美国新泽西州
[72]发明人 马克·H·埃特塞尔
罗伯特·约汉·弗兰克
丹尼尔·尼尔森·西尔
罗伯特·约汉·奈克内里斯
西姆扬·B·米兹科夫斯基
罗伯特·约汉·兰斯 R·戴尔·西普

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 蒋世迅

权利要求书6页 说明书11页 附图页数7页

[54]发明名称 改善无线电话消息安全性用的多重CMEA迭代加解密的方法和装置

[57]摘要

适合应用于无线电话的一种增强式CMEA加密系统。明文消息输入至系统中，经受应用第一CMEA密钥进行的第一次CMEA迭代处理，产生一个中间密文。然后，中间密文经受应用第二CMEA密钥进行的第二次CMEA迭代处理，产生出最后的密文。在每次CMEA迭代处理之前和之后使明文和中间密文经受输入和输出变换以达到附加的安全性。CMEA迭代可以采用改善的tbox函数应用来实施，tbox函数对消息或中间加密处理的数据附加以置换。实现解密时使密文消息经受与加密中所使用步骤相反次序的步骤，将输入和输出变换分别用合适的反输出和反输入变换来代替。

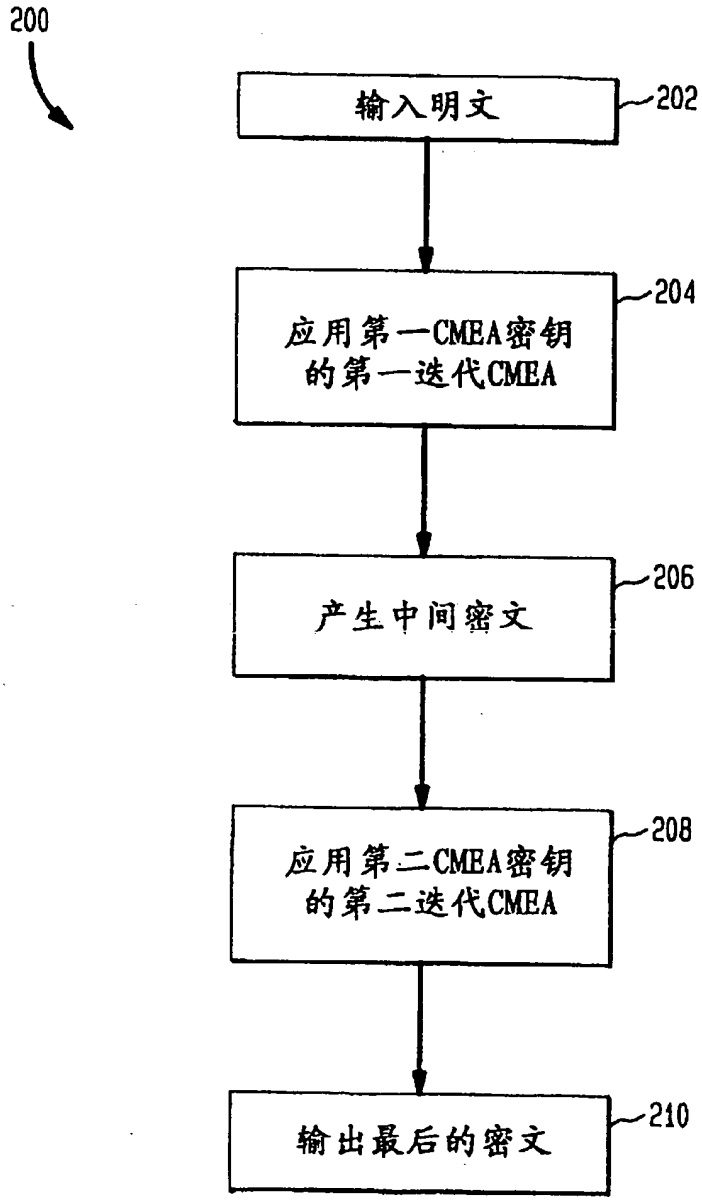
ISSN1008-4274

第二次 CMEA 迭代处理之后，执行第二输入变换和第二输出变换。按照本发明的另一种加密系统，可取地通过在一次或多次 CMEA 迭代处理中附加上至少一次 tbox 的输入置换，以改善 tbox 函数的应用。该改善的 tbox 函数的应用公布在我们的相关专利申请，名称为“改善无线电话消息安全性用的、使密钥扩展入查找表内以增强安全性的方法和装置”中，它与本专利申请在同一日申请，在此引入作为参考。本发明的另一个方面中，可实施第一和第二次 CMEA 迭代处理，但在每一次 CMEA 迭代处理之前和之后不作输入和输出变换。

图 2 是一个流程图，示明按照本发明之另一个方面由加密处理 200 实施的步骤。图 2 的加密处理中包括了与图 1 的论述中关联的 CMEA 迭代处理共两次，每一次迭代中采用了不同的 CMEA 密钥。在步骤 202 上，将明文引入至加密处理中。在步骤 204 上，应用第一 CMEA 密钥的 CMEA 处理，于第一次迭代中将明文加密。在步骤 206 上，完成第一次迭代，产生出中间密文。在步骤 208 上，应用第二 CMEA 密钥的 CMEA 处理，使中间密文经受第二次迭代。在步骤 210 上，产生出最后的密文。

图 3 是一个流程图，示明按照本发明之另一个方面的加密处理 300。在步骤 302 上，将明文消息引入至加密处理中。在步骤 304 上，明文消息经受第一输入变换，产生出经第一输入变换的消息。在步骤 306 上，应用第一 CMEA 密钥使第一输入变换的消息经受第一次 CMEA 迭代处理，产生出第一中间密文。可取地，第一次 CMEA 迭代处理中使用了改善的 tbox 函数应用，在其中， tbox 函数的每一次输入经受一次置换。该改善的 tbox 函数应用公开于我们上述的相关专利申请中。在步骤 308 上，第一次 CMEA 迭代处理的输出经受第一输出变换，产生出经第一输出变换的消息。在步骤 310 上，第一中间密文经受第二输入变换，产生出经第二输入变换的消息。在步骤 312 上，应用第二 CMEA 密钥使变换出的中间密文经受第二次 CMEA 迭代处理，产生出第二中间密文。

图2


200
输入明文
202
应用第一CMEA密钥的第一迭代CMEA
204
产生中间密文
206
应用第二CMEA密钥的第二迭代CMEA
208
输出最后的密文
210